

EXHIBIT 2

Declaration of Kevin Skoglund – 02/20/24

***PLAINTIFFS' MOTION FOR SANCTIONS AGAINST DEFENDANTS
CCBOER AND COUNSEL***

CGG, et al. v. Coffee Cty. Bd. of Elections and Registration
United States District Court for the Southern District of Georgia
No: 5:23-mc-00001-LGW-BWC

**IN THE UNITED STATES DISTRICT COURT FOR
THE SOUTHERN DISTRICT OF GEORGIA
WAYCROSS DIVISION**

**COALITION FOR GOOD
GOVERNANCE and DONNA
CURLING,**

Plaintiffs,

v.

**COFFEE COUNTY BOARD OF
ELECTIONS AND REGISTRATION,**

Defendant.

**Civil Action No.: 5:23-mc-00001-
LGW-BWC**

**In RE Subpoenas issued by the
United States District Court
For the Northern District of
Georgia, Atlanta Division,
Civil Action File No. 1:17-
CV-2989-AT**

DECLARATION OF KEVIN SKOGLUND

Pursuant to 28 U.S.C. § 1746, I, KEVIN SKOGLUND, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of all facts stated in this declaration, and if called to testify, I could and would testify competently thereto.
2. The Coalition for Good Governance has retained me as a technical expert.
3. I am a testifying expert for Coalition for Good Governance in the Curling v. Raffensperger case. I testified at the trial in January 2024. The Court accepted me as an expert in election security, cybersecurity, and election technology. The

75-page declaration containing my summary and analysis of evidence related to events in Coffee County, Georgia was admitted into evidence at trial.¹

4. In the course of developing that declaration, I attended thirteen depositions via video conference between July 2022 and November 2022 that were related to Coffee County. I reviewed all of the documents produced by the deponents. I conferred with the attorneys about the documents, deposition questions, and testimony.

5. On November 20, 2023, attorneys for the Coalition for Good Governance provided me with a forensic image² made by the Georgia Bureau of Investigation (“GBI Image”). It is my understanding that the GBI Image was made from a desktop computer used by the Coffee County Supervisor of Elections.

6. The attorneys asked me to conduct a search for documents that might have been responsive to prior subpoenas and Open Records Requests (“ORRs”) served on Coffee County by Coalition for Good Governance. I was already familiar with the nature of the documents being sought based on my prior data analysis, but I was also provided the subpoenas, ORRs, and key word search terms as reference.

7. The attorneys for the Coalition for Good Governance advised me that—because of the nature of the original computer—the GBI Image might contain

¹ Exhibit A: December 5, 2022 Declaration of Kevin Skoglund

² The forensic image was created by “DFI Morton” on July 17, 2023 and has a SHA value of 8c4db97f78a54540229638992f3223bc56b8dcd.

information about voters, personal documents belonging to the current or past Supervisors of Elections, or other private or privileged material. The attorneys asked me to seek their approval for any documents with potential sensitivities before sharing them with the plaintiffs.

8. Therefore, I adopted a process to filter documents first based on likely responsiveness (i.e., all documents that matched a keyword search), and then to review the full content of each of those documents to filter them for potential sensitivities. The requirement to filter for sensitive information added significant time to my search process. I observed the presence of many sensitive documents during my search, but none were included in the responsive documents.

9. I opened and extracted data from the forensic image using Autopsy, a software program commonly used for working with forensic images. Autopsy allows one to browse, search, and copy files without modifying any data on the original image.

10. The first task I undertook was to locate any email files. Plaintiffs had advised me that Coffee County had stated several times that no email files existed for Misty Hampton, the Supervisor of Elections up until February 2021, because her Microsoft Outlook account had been deleted after her departure.

11. Coffee County's statement was false. The emails for Misty Hampton, James Barnes, and Rachel Roberts were located exactly where any IT

professional would expect to find them and easily discovered by anyone who put in a small amount of effort to search for them.

12. Microsoft Outlook stores emails for each user in an OST file that ends in “.ost”. The default location for an OST file is in the user’s home directory, inside the directories “AppData\Local\Microsoft\Outlook”. If one did not know that location already, one could search the internet for “how to find Outlook files” to quickly find a Microsoft Support article that explains: “The offline Outlook Data File (.ost) is also saved at drive:\Users\user\AppData\Local\Microsoft\Outlook.”³

13. The Outlook file for Misty Hampton contained 8,572 emails. The Outlook file for James Barnes contained 2,208 emails. The Outlook file for Rachel Roberts contained 2,560 emails. My review of these three accounts, with over 13,000 emails total, located approximately 1,000 emails that were responsive to the search. Many were important to the Curling case, and the Plaintiffs had never seen them before.

14. The second task I undertook was to locate any documents on the hard drive. I found thousands of documents in the user home directories of Misty Hampton, James Barnes, and Rachel Roberts. I found approximately 145 documents that were responsive to the search. Many were important to the Curling case, and the Plaintiffs had never seen them before.

³ <https://support.microsoft.com/en-us/office/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790>

15. I found that Misty Hampton deleted many files on the day of her departure. These file were recovered using Autopsy and would have been recoverable using any other IT file recovery software. Deleted files typically remain on a hard drive and are recoverable until another file is saved to that same hard drive location, overwriting it. It cannot be known whether continued daily use of the computer caused it to overwrite other deleted files so that they are no longer available. An earlier recovery effort might have discovered more.

16. There is evidence on the GBI Image that indicates that additional documents may still reside on a networked server in Coffee County's possession or control. There are many forensic artifacts—such as email attachments, links to recent documents, and PDF files opened in a browser—that reference documents located on a networked server. The references start with the file path: “file://cc-ch-fs01/UserData/Coffee County/Elections/Old Data from FS03/Misty/” The next directory in that path is usually “2019” or “2020”, which suggests that this directory was not exclusively used for “Old Data”.

17. One document, “Letter NOT Certifying Recount.docx”, was of particular interest to the Plaintiffs. It was emailed to Preston Haliburton on December 31, 2020 and has been cited as the “invitation” for outsiders to come to Coffee County in January 2021. Misty Hampton's email account includes one version of the document as an attachment to a sent email. The GBI Image does not contain the original Microsoft Word document or any other versions, but it does contain a

reference to a document on the networked server, “[...]/Old Data from FS03/Misty/”. In addition, other emails contain a reference to a *different* document, one with the same title but with different content, which also resides on that networked server.

18. I spent approximately 58 hours reviewing and filtering the contents of the GBI Image at a rate of \$500 per hour. This time is in addition to the many hours spent attending depositions, reviewing deponent documents, and conferring with the Plaintiffs and attorneys. I will be working with the attorneys at their request over the next several days to analyze and categorize the hours devoted to those breach-related discovery activities. Such hours will be reported on a supplemental declaration.

Executed on this date, February 20, 2024.

A handwritten signature in black ink, reading "Kevin Skoglund", written over a horizontal line.

Kevin Skoglund

Declaration of Kevin Skoglund - December 5, 2022
EXHIBIT A

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, et al.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, et al.,
Defendants.**

Civil Action No.: 1:17-cv-2989-AT

DECLARATION OF KEVIN SKOGLUND

Pursuant to 28 U.S.C. § 1746, I, KEVIN SKOGLUND, declare under penalty of perjury that the following is true and correct:

1. This declaration supplements my declarations previously submitted in this case, and I incorporate my previous declarations as if fully stated herein.

2. The Court has acknowledged my role as a voting system security expert engaged by Coalition Plaintiffs to provide expert analysis and testimony on the security and technical aspects of Georgia's voting system.

3. In January 2021, several individuals were given irregular access to the Coffee County Election Office and to Georgia's voting system in Coffee County.

4. Coalition Plaintiffs asked me to examine the documentary evidence of the irregular access to the Coffee County Election Office and its election equipment to determine what activities took place, to determine what election software or data

may have been copied and distributed, and to assess the implications of my findings.

5. Coalition Plaintiffs provided me with extensive data, documents, and security camera video recordings produced under subpoena for my analysis, which I reviewed thoroughly. Coffee County Election Office security video was produced by Coffee County counsel to Plaintiffs' counsel. The video recordings cover the time period from November 15, 2020 to February 26, 2021 and include three camera views: the primary outside entrance, the foyer and main room inside the Election Office, and a storage room. Throughout my declaration I have referenced video footage based on the date and time stamps in the video recordings. I believe the date and time stamps to be accurate. The video recordings are voluminous and cannot be easily transmitted online. The recordings will be made available to the Court upon request. They are available to the public upon request from Coffee County as public records.

6. I attended all of the depositions related to Coffee County via video conference and reviewed the transcripts. My analysis relies on the totality of this information and cites select items when appropriate.

7. Coalition Plaintiffs' counsel represented to me that some documents responsive to subpoenas have yet to be produced by the witnesses. When those documents become available, my declaration may require supplementation.

8. I had prior information about many of the individuals involved, their affiliations, and their election-related activities outside of Georgia, primarily through press reports and court filings. I used this knowledge during my analysis, but I primarily cite facts in the evidence for this case.

I. Summary of Conclusions

9. After a review of the documentary evidence, my primary findings and conclusions are:

a. In 2021, the security of Georgia's voting system was breached in Coffee County on at least three occasions: January 7, January 18-19, January 25-29.

b. On January 7, four SullivanStrickler employees travelled to the Coffee County Election Office. Over a seven-hour period, they copied data from much of the election hardware using forensic tools and techniques. They left Coffee County with election software and data on a hard drive. At least seven individuals—including one Election Board member and the Election Director—were concurrently in the Election Office. SullivanStrickler performed the data collection under a contract signed by Sidney Powell on behalf of Defending the Republic, and were paid by Defending the Republic PAC. Their work was directed or coordinated by at least ten individuals.

c. The data collected by SullivanStrickler included complete copies of software and data from a variety of election devices. Four significant election components were included: the Election Management System server, the ImageCast Central scanner/tabulator, the ImageCast X ballot marking devices, and the media used to program ImageCast Precinct scanners.

d. Coffee County election software and data was distributed to at least ten individuals between January and June 2021. These individuals are affiliated with at least seven different organizations. Evidence suggests it was distributed further by some of those individuals.

e. During January 18-19, 2021, Doug Logan and Jeffrey Lenberg were given extraordinary access to Georgia's voting system in Coffee County by the Election Director. They had access for over 13 hours, including hours when the Election Office was closed to the public. During their visit, the system dates on several election computers were changed, scanner settings were reconfigured several times, over 6,500 ballots were scanned, and one precinct scanner was opened up to inspect the parts inside. Their work was organized by James Penrose and Charles Bundren.

f. During January 25-29, Jeffrey Lenberg was again given extraordinary access to Georgia's voting system in Coffee County by the

Election Director. He had access for almost seven hours over five days, and indicated an intention to have significantly more. During his visit, the system date on the central vote tabulator was changed twice (and never changed back), media was created to program a precinct scanner and a ballot marking device, 559 ballots were scanned, and he was given voting system data to take with him.

g. I am aware of no authorization given for the irregular access to Coffee County's Election Office in January 2021. The evidence indicates an illusion of authorization was created (1) by Eric Chaney leveraging his membership on the Board of Elections, (2) by Misty Hampton's willingness to collaborate, (3) by several attorneys lending their integrity as officers of the court, and (4) by involving many other willing and credulous participants.

h. These events were by any measure a consequential breach of Georgia's election security. The access controls to protect election hardware and software were obviously insufficient. The data collected includes protected software from almost every component of Georgia's election system. Control over the software and data cannot be reestablished after its distribution, and all of Georgia's counties and other states must endure the increased risks as a result.

i. The distribution of the data from Coffee County has made it easier for adversaries to obtain Georgia’s election software, which expands opportunities for existing and new adversaries. Those adversaries may use the software in disinformation campaigns or study it to learn how to subvert its operation through malware, reprogramming, or disabling defenses. This breach and others like it portend easier access to equipment to put manipulations into effect—in Coffee County strangers were given free rein for hours. These implications require that the recommendations of election security experts should be implemented fully and urgently.

10. Below, I will address each of these conclusions in greater detail.

II. Activity Related to Access on January 7, 2021

11. On the Signal messaging application, a message group titled “SullivanStrickler” was used by several employees of SullivanStrickler, a company in the Atlanta area which offers forensic data services.¹ The message group participants included Paul Maggio, Greg Freemyer, Jennifer Jackson, and Karuna Naik. On January 1, 2021 at 2:18pm, Jennifer Jackson forwarded a text message to her colleagues from “Katherine”: “Hi! Just handed [sic] back in DC with the Mayor. Huge things starting to come together! Most immediately, we were granted access -by written invitation! - to the Coffee County Systems [sic]. Yay! Putting

¹ SullivanStrickler corporate website, <https://www.sullivanstrickler.com>

details together now with Phil, Preston, Jovan etc. Want to give you a heads up for your team. [...]”²

12. In subsequent Signal messages during January 1-5, SullivanStrickler colleagues relayed updates about scheduling work in Coffee County based on various communications with Preston Haliburton and “Todd”.³

13. Because of SullivanStrickler’s communications with Haliburton, I found it relevant that on the prior day, on December 31, 2020 at 7:46pm, Eric Chaney, a Coffee County Election Board member, texted Misty Hampton, the Coffee County Election Director: “Did you get the letter sent”. Hampton replied, “No. I am going to finish it tomorrow”. Chaney responded with Preston Haliburton’s email address. At 9:13pm, Hampton texted back, “I resent it” and Chaney answered, “Thanks!!”⁴

14. If a “letter” from Hampton to Haliburton was the “written invitation” touted in Katherine’s message the following day, it was not in the evidence I reviewed.

15. On January 6, 2021 at 4:26pm, Hampton texted Chaney: “Scott Hall is on the phone with Cathy about wanting to come scan our ballots from the general election like we talked about the other day. I am going to call you in a few”.⁵

Security camera video shows Hampton and Cathy Latham, the chair of the Coffee

² Exhibit 1, SSA Signal Messages, p. 1

³ Ibid, p. 4-12

⁴ Exhibit 2, Hampton-Chaney Messages - Dec 2020, p. 1

⁵ Ibid, p. 2

County Republican Party, were together in the Election Office at that time, and shows Latham using a cell phone several times.

16. On or around January 6, 2021, a group message was created on Signal, titled “Coffee_County_Forensics”. The participants were James Penrose, Paul Maggio (SullivanStrickler), Greg Freemyer (SullivanStrickler), Jim Nelson (SullivanStrickler), Scott Hall, and attorney Charles Bundren. At 7:35pm, Penrose introduced Hall to the SullivanStrickler team. Bundren responded, “We need cell numbers to identify who they are for the people at the elections HQ.” After phone numbers are exchanged, Maggio requests, “Please provide address and POC [point of contact] name and phone”. Just after midnight, on January 7 at 12:21am, Hall responds, “Important to text POC Before coming in. [...] / POC is Mitzi Martin⁶ Supervisor of Elections [...] / Second POC is Cathy Latham [...]” At 5:04am, Maggio responds, “We are planning on driving down. Leaving Atlanta around 8 AM”.⁷

17. On January 7, 2021 at 10:31am, Paul Maggio (SullivanStrickler) emailed Sidney Powell, an attorney, and copied James Penrose, Doug Logan, Tricia (Powell’s associate), and Brendan Sullivan (SullivanStrickler). The subject was “RE: SSA1722: Jim Penrose - Coffee County GA Forensics Engagement

⁶ Misty Hampton’s surname was Martin at the time.

⁷ Exhibit 2, SSA Signal Messages, p. 17-20

Agreement”. Maggio wrote: “Per Jim Penrose’s request, we are on our way to Coffee County Georgia to collect what we can from the Election / Voting machines and systems. As per our existing agreement, I am attaching the invoice for our initial retainer.”⁸

18. The invoice attached to the email was dated January 7, 2021 and billed to Sidney Powell / Defending the Republic, for project SSA1722 in the matter of “Voting Machines Analysis”. The two line items are “Forensics: Forensic Expert Daily Rate; 01/07/2021 On Site Coffee County Georgia; 4 people x 1 day” and “Forensics:Travel; Mileage | 394 miles round trip Atlanta GA to Douglas GA”. The total balance due is \$26,220.64.⁹

19. Earlier emails indicate that Maggio’s reference to “our existing agreement” pertains to the Engagement Letter, drafted by Maggio and signed by Powell on behalf of Defending the Republic on December 6, 2020.¹⁰ Exhibit 1 to the Engagement Letter states “Customer is requesting that SS provide services such as Computer Forensic Collections and Analytics on the Dominion Voting Systems equipment; from the Poll Pads (iPads) to the Windows machines that run the scanners, to Linux machines that tabulate the votes [...]”¹¹

⁸ Exhibit 4, Maggio email to Powell en route

⁹ Exhibit 5, SSA Invoice

¹⁰ Exhibit 6, SSA - Powell Engagement Letter

¹¹ Ibid, p. 3

20. On January 7, 2021 between 11:09am and 11:42am, text messages between Cathy Latham and Scott Hall coordinated SullivanStrickler's arrival.¹² Latham also texted Maggio: "How far out are you?" Maggio responded with "We are in town waiting for Scott to let us know when to pull in."¹³

21. Security camera video shows Latham waited outside the Coffee County Election Office at that time. When Paul Maggio, Jennifer Jackson, and Jim Nelson from SullivanStrickler arrived at 11:43am, Latham greeted them, escorted them inside, and introduced them to Misty Hampton (Election Director), Eric Chaney (Election Board member), and Ed Voyles (a former Election Board member with no official relationship to the Election Office at the time).

22. Security camera video shows Latham exited the Election Office and waited outside again. At 11:50am, Scott Hall and Alex Cruce arrived. Scott Hall is a bail bondsman from Atlanta, and Alex Cruce is a data analyst. They flew to Coffee County together on a private jet arranged by Hall.¹⁴ Latham escorted them inside and introduced them.

23. Over the next hour, the SullivanStrickler team met with the assembled group in Hampton's office, retrieved equipment from their car, and were joined by their late-arriving colleague, Karuna Naik.

¹² Exhibit 7, Latham-Maggio Messages, p. 2

¹³ Exhibit 7, Latham-Maggio Messages, p. 1

¹⁴ Alex Cruce Deposition Tr:152:13

24. Security camera video, photographs taken by SullivanStrickler, and metadata in files produced by SullivanStrickler agree that, over the next seven hours, the SullivanStrickler team made copies of the electronic data on much of Coffee County's election equipment using forensic tools and techniques.

25. A photograph produced by SullivanStrickler shows a Dell Precision 3431 computer inside the server room in the Coffee County Election Office.¹⁵ The computer monitor has a black screen with white text, not the typical Windows operating system. One of the computer's USB ports is connected to a WD MyPassport external hard drive via a cable. The USB port above it is occupied by a USB drive with a manila hang tag labeled "DFIR UEFI".

26. DFIR is an abbreviation for "digital forensics and incident response." Digital forensics is a cybersecurity field that examines computer data, frequently through the creation of forensic images.

27. UEFI is an abbreviation for "Unified Extensible Firmware Interface." UEFI can be thought of as a tiny operating system that runs on a computer instead of a standard operating system, like Microsoft Windows. UEFI is a common digital forensics tool for creating forensic images without activating the operating system on the target device.

¹⁵ Exhibit 8, SSA Photographs - Dell computer, p. 1

28. Another photograph produced by SullivanStrickler shows team members Jim Nelson and Karuna Naik working at the same Dell Precision 3431 computer while it is booted from the UEFI USB drive for the purpose of making a forensic image on the external hard drive.¹⁶

29. A third photograph produced by SullivanStrickler shows a Dell Latitude 3400.¹⁷ Its screen reports that the creation of a forensic image is 67% complete. Plugged into the left side of the laptop is the USB drive tagged “DFIR UEFI” and a USB cable, presumably connected to an external hard drive out of frame.

30. It is a best practice in digital forensics to use a write-blocker when connecting any external device to the device being examined or copied. A write-blocker allows reading data *from* a device but prevents sending data *to* a device. Because data can only travel out, it precludes any data modification. It is possible to work without a write-blocker and not modify any data, but a write-blocker protects the device from mistakes by the technician and from any malware resident on the external device.

31. SullivanStrickler agreed that using a write-blocker is a best practice.¹⁸ However, a write-blocker was not used in Coffee County. A hardware write-blocker—a device slightly larger than a bar of soap—is not visible in the

¹⁶ Exhibit 8, SSA Photographs - Nelson and Naik, p. 2

¹⁷ Exhibit 8, SSA Photographs - Dell Laptop, p. 3

¹⁸ Dean Felicetti Deposition Tr: 224:4-225:15

photographs. More importantly, I reviewed evidence in the data collected by SullivanStrickler that their activity *did change* data on one of the devices.

32. The Windows operating system records the connection of any USB device by default. In the data collected by SullivanStrickler, the relevant records¹⁹ show that at 12:30pm, two USB devices were connected to the Election Management System server (“EMS”). The first was a WD MyPassport external hard drive, model WDBPKJ, serial number 575855324139303037584655. The second was a Samsung USB Drive, serial number 0376220080003100. These USB devices are consistent with the USB devices in the photographs.

33. In my opinion, this data change on the target device was likely due to a mistake by a technician. The EMS was the first device copied and the mistake was not repeated on other devices. I cannot determine if this mistake resulted in additional changes to the EMS because the only available evidence is from data captured *after* these USB connections were made. I can only conclude that a write-blocker was not used and at least some data on the EMS was changed as a consequence.

34. At 2:56pm, Maggio updated Penrose and Bundren via the “Coffee_County_Forensics” Signal group. “Collection is going well. No real issues

¹⁹ Windows Registry Key: HKLM\SYSTEM\ControlSet001\Enum\USB\

at this point. Looking to be here until 6-7 PM this evening”. Bundren replied with, “Thanks”.²⁰

35. Security camera video of the primary room in the Election Office shows SullivanStrickler personnel engaged in activities consistent with copying data from KNOWiNK Poll Pads and USB drives. Security camera video did not include a view inside office of the Election Director or the server room beyond it where other election equipment resides.

36. Security camera video shows the SullivanStrickler team and everyone else departed the Election Office together at 7:43pm. At 7:47pm, Maggio updated the Signal group again, “We just finished up at Coffee County and are on our way back to Atlanta. Everything went well with no issues.” Bundren responded, “Thanks”, and Hall responded with emojis for thank you and the American flag.²¹

37. On January 8 at 3:48pm, Maggio replied to his prior email to Sidney Powell and added Scott Hall’s email address to the copied recipients list. Maggio wrote: “Everything went smoothly yesterday with the Coffee County collection. Everyone involved was extremely helpful.” He raised the issue of payment, then continued, “We are consolidating all of the data collected and will be uploading it to our secure site for access by your team.”²²

²⁰ Exhibit 1, SSA Signal Messages, p. 21

²¹ Exhibit 2, SSA Signal Messages, p. 22

²² Exhibit 8, Maggio-Powell Email - Jan 7

38. On January 9 at 5:24pm, Maggio sent Freemyer a message on Signal, “We are not uploading/giving access to anyone until we are paid. / I am communicating with Jim P one on one on Signal about getting paid before we release any data”. A few hours later, Maggio updated Freemyer, “Greg, let’s keep communications quiet for now. I am now negotiating directly with Sidney”.²³

39. For this portion of my analysis I concluded:

a. On January 7, four SullivanStrickler employees—Paul Maggio, Jennifer Jackson, Jim Nelson, and Karuna Naik—travelled to the Coffee County Election Office. Over a seven-hour period, they copied data from much of the election hardware using forensic tools and techniques. They left Coffee County with election software and data on a hard drive.

b. While SullivanStrickler worked, at least seven individuals were concurrently in the Election Office: Eric Chaney (Election Board member), Misty Hampton (Election Director), Jil Ridlehoover (Assistant to the Election Director), Cathy Latham, Ed Voyles, Scott Hall, Alex Cruce.

c. SullivanStrickler performed the data collection under a contract signed by Sidney Powell on behalf of Defending the Republic, and were paid by Defending the Republic PAC. Their work was directed or coordinated by Sidney Powell, “Katherine”, Preston Haliburton, “Todd”,

²³ Exhibit 1, SSA Signal Messages, p. 24

James Penrose, Charles Bundren, Scott Hall, Cathy Latham, Eric Chaney, Misty Hampton, and other individuals.

III. Coffee County Data Collected by SullivanStrickler

40. I examined a physical hard drive produced by SullivanStrickler which SullivanStrickler represented contained all data collected in Coffee County on January 7, 2021 (“SSA Hard Drive”). The SSA Hard Drive has several directories which contain forensic images.

41. A forensic image is a copy of a physical data storage device which copies every data bit exactly as it exists on the device, including all directories, all files, and currently unallocated storage (which may include previously deleted data). A forensic image has significantly more fidelity to the original device than a copy made by dragging directories and files to a new device. It is an exact copy.

42. The SSA Hard Drive has forensic images of a Dominion Democracy Suite Election Management System server (“EMS”) from Coffee County as it existed on January 7, 2021. Coffee County’s EMS has two hard drives inside²⁴ and both were copied.

43. The EMS is a central computer with two important functions. Before an election, the EMS configures data for each election—precincts, ballot styles,

²⁴ Dell Support Website, Service tag BRKP513, <https://www.dell.com/support/home/en-us/product-support/servicetag/0-UnNYXXRjckNITU1WanA0UXJNdUImdz090/overview>

contests, candidates, layout—which is then used to program scanner/tabulators and ballot marking devices. After an election, the EMS manages the import of data from all of the tabulators, aggregates the subtotals for each contest, and creates reports of the election results. The EMS is the most important component in the election system because it is responsible for both establishing the election “rules” and determining the election results.

44. The SSA Hard Drive has a forensic image of a Dominion ImageCast Central scanner/tabulator (“ICC”) from Coffee County as it existed on January 7, 2021.²⁵

45. An ICC is commonly used to scan and tabulate ballots returned to the election office by mail.

46. The SSA Hard Drive has forensic images of 18 CompactFlash cards used with Dominion ImageCast Precinct scanner/tabulators from Coffee County as they existed on January 7, 2021.

47. CompactFlash cards are used by the Dominion ImageCast Precinct scanner/tabulators (“ICP”). The EMS exports data about an election, specific to each ICP, onto a CompactFlash card. The card is inserted into a port on an ICP, where it remains during voting. The card provides the ICP with data about the election, ballots, contests, candidates, and other configurations. When the polls

²⁵ The SSA Hard Drive directory containing the forensic image of the ICC is mislabeled as “ICP”.

close, the card will contain post-election data such as the tabulation results, cast vote records, ballot images, and log files. After the card is returned to the election office, the EMS can extract the tabulation results and other data from it.

48. Photographs produced by SullivanStrickler show 18 CompactFlash cards with labels corresponding to ICPs in each of Coffee County's six precincts and early voting sites.²⁶ The text "March 24 2020 PPP" also appears, but is no longer correct because the cards have been reused since the label was printed.

49. I examined the contents of these 18 forensic images. At the time they were copied, the CompactFlash cards held data from the 2021 Run-off Election that had just concluded on January 5, 2021. The forensic images include ICP scanner configuration data, election results, image files of the ballots scanned during the 2021 Run-off Election, and residual ballot images from the 2020 General Election which were not overwritten by new data when the cards were reused.

50. The SSA Hard Drive has forensic images of seven USB drives from Coffee County as they existed on January 7, 2021.

51. USB drives are used by a Dominion ImageCast X ballot marking device ("ICX") in two ways. First, USB drives are used to install Dominion software on an ICX. Second, USB drives provide an ICX with data about the election, ballots,

²⁶ Exhibit 08, SSA Photographs - CompactFlash cards, p. 4-5

contests, candidates, and other configurations. This data controls the content on the ICX touchscreen and controls the content of the QR code and text on ballots printed by the ICX.

52. Photographs produced by SullivanStrickler show seven USB drives with labels.²⁷ One forensic image, created from the USB drive labeled “ICX install”, contains two versions of the Android software used by the ICX, versions 5.5.10.30 and 5.5.10.32.²⁸ The six other forensic images contain data used to program an ICX for four previous elections.

53. The SSA Hard Drive also has a forensic image of a Mobile Ballot Printing laptop, partial data from 20 KNOWiNK Poll Pads, election-related reports for the 2020 General Election and 2021 Run-off Election, and scanned images of ballots from the 2021 Run-off Election.

54. For this portion of my analysis I concluded:

The data collected by SullivanStrickler included complete copies of software and data from a variety of election devices. Four significant election components are included: the Election Management System server, the ImageCast Central scanner/tabulator, the ImageCast X ballot marking devices, and the media used to program ImageCast Precinct scanners.

²⁷ Exhibit 8, SSA Photographs - USB drives, p. 6-7

²⁸ On October 4, 2020, I submitted a declaration (Doc. 943) regarding the hasty upgrade from Dominion Democracy Suite ImageCast X 5.5.10.30 to 5.5.10.32. It is my understanding the newer version was installed on every ICX in Georgia later that month.

IV. Distribution of Coffee County Data

55. After its collection, Coffee County election software and data was distributed on at least three occasions: January 2021, April 2021, June 2021.

Distribution via ShareFile in January 2021

56. On January 8, 2021, Maggio emailed Powell, “We are consolidating all of the data collected and will be uploading it to our secure site for access by your team.”²⁹ The “secure site” is a ShareFile account maintained by SullivanStrickler. ShareFile is a popular, internet-based file storage and sharing platform operated as a service by a third party, Citrix Systems.³⁰ Administrators of an account can grant users permission to access certain directories. Users of the service can upload and download files in those directories through a public website.

57. Exhibit 10 (“ShareFile Permissions”) shows which users SullivanStrickler granted permission to view, upload, download, or delete files in specific directories on their account.³¹ Exhibit 11 (“ShareFile Log”) is a list of activity showing each upload or download by a user who has been granted permissions.³² Each entry in the log shows the date and time, file path, logged in user’s name, email, company, IP address, and other information. The entries are in reverse chronological order, with the oldest entries at the bottom. Portions of the

²⁹ Exhibit 9

³⁰ Citrix Systems ShareFile product website, <https://www.sharefile.com>

³¹ Exhibit 10, ShareFile Permissions (with redactions)

³² Exhibit 11, ShareFile Log (with redactions)

ShareFile Permissions and ShareFile Log were redacted in the image and PDF versions, but the text versions are unredacted.³³

58. ShareFile Log shows that Paul Maggio created a new directory on ShareFile on January 9, 2021 at 1:21pm, named “SSA1722/Coffee County Data”. ShareFile Permissions shows this new directory allowed eight SullivanStrickler employees, Doug Logan, Todd Sanders, Conan Hayes, and James Penrose to upload and download files.

59. Doug Logan is listed with an email address at “fightback.law”, a domain associated with #FightBack Foundation, Inc, which is operated by Lin Wood.³⁴ Logan does not have a company listed, but he was the owner of CyberNinjas.³⁵ Todd Sanders is listed as “Scott T”, however the email address listed at “bonfiresearch.org” belongs to Sanders.³⁶ His company is “ASOG”, an abbreviation for Allied Security Operations Group.³⁷ Conan Hayes has an email address at “bonfiresearch.org” and his company is also “ASOG”. James Penrose has an email address at “fightback.law” and his company is Defending the

³³ Exhibit 12, ShareFile Permissions and Log (no redactions), (Linked at <https://www.dropbox.com/s/gqlxtxuezipwxx/08122022-000137.txt>)

³⁴ #FightBack Foundation website, <https://www.fightback.law>

³⁵ Doug Logan Deposition Tr: 5:8

³⁶ Doug Logan confirmed the email address belonged to Todd Sanders. Doug Logan Deposition, Tr 97:2-3

³⁷ Allied Security Operations Group corporate website, <https://asog.us>

Republic, the organization affiliated with Sidney Powell which paid SullivanStrickler for the Coffee County data acquisition.

60. Logan, Sanders, Hayes, and Penrose already had access to SullivanStrickler’s ShareFile account prior to January 9. They had previously collaborated with SullivanStrickler on the acquisition of election software and data from Antrim County, Michigan.³⁸ ShareFile Permissions shows they had access to other directories related to that work, and ShareFile Log lists earlier file uploads and downloads by them related to that work.³⁹

61. ShareFile Log shows that, after creating the “Coffee County Data” directory, Maggio uploaded all of the data acquired in Coffee County into it in several sessions during January 9-12. A few hours after he began uploading files, Logan, Sanders, and Hayes began downloading the same files.

62. Then, on January 10, Doug Logan created a new directory on ShareFile, “SSA1722/DJL Upload/Coffee – EMS.” It is notable that this new directory *was not inside* the “Coffee County Data” directory created by Maggio. ShareFile Log shows that the “DJL Upload” directory had existed since December 31, 2020. ShareFile Permissions shows it had the same permissions as the “Coffee County

³⁸ Exhibit 13, Plaintiff’s First Amended Expert Witness List. *Bailey v. Antrim County*, Michigan Circuit Court for the County of Antrim, Case No. 20-9238-CZ. Apr. 9, 2021 2021. Proposed expert witnesses include many individuals involved in Coffee County: James Penrose, Ben Cotton, Doug Logan, Greg Freemyer, Paul Maggio, Phil Waldron, Russ Ramsland, Jeffrey Lenberg, Todd Sanders, Conan Hayes.

³⁹ These entries are redacted in the image and PDF versions but are unredacted in the text versions.

Data” directory—eight SullivanStrickler staff, Logan, Sanders, Hayes, Penrose—with one notable addition. Michal Pospieszalski from Mehow Consulting, LLC, with an email address at “exemplarbusiness.com”, had permission to upload and download files.⁴⁰

63. ShareFile Log shows that, early on January 11, Logan began uploading files to the “SSA1722/DJL Upload/Coffee – EMS” directory. Logan testified that “I converted the forensic image into a virtual machine, and I uploaded that result to the site. [...] [C]onverting it to a virtual machine allows you to potentially, you know, boot up the device and be able to utilize it like a computer, in order to look at how things operate, and more closely examine it like it was a local system you were using.”⁴¹ In other words, Logan uploaded a new version of the forensic image that could be used more easily for analysis. Todd Sanders downloaded the virtual machine files the same morning.

64. On January 13, Doug Logan created a new directory on ShareFile, “SSA1722/DJL Upload/Coffee – ICC” and uploaded similar virtual machine files to it. Conan Hayes began downloading the files immediately.

65. The same day, James Penrose downloaded all files in the directory “SSA1722/Coffee County Data/Coffee County Ballot Images”.

⁴⁰ These entries are redacted in the image and PDF versions but are unredacted in the text versions.

⁴¹ Doug Logan Deposition Tr: 111:19-112:8

66. On January 15, Doug Logan created a new directory on ShareFile, “SSA1722/DJL Upload/Coffee – EMS – Fixed,” and uploaded files to it. When asked about this version, Logan testified, “the first time I did the conversion, something happened, and [...] it didn’t actually function and work right. [...] I redid a process and uploaded a version that actually functioned.”⁴² Todd Sanders downloaded the updated virtual machine files during January 18-19.

67. On January 19, Michal Pospieszalski downloaded all files in the directory “SSA1722/DJL Upload”.⁴³ The download would have included among its contents the three directories added by Logan—“Coffee – EMS”, “Coffee – ICC”, “Coffee – EMS – Fixed”—which contained virtual machines of the EMS and ICC.

68. The ShareFile Log ends on February 26 which was on or around the date the document was generated from ShareFile. SullivanStrickler testified that the files remained on ShareFile until “Summer of 2021”⁴⁴ but that additional activity, which is now over a year ago, is not visible in their ShareFile account.⁴⁵

69. [REDACTED] Jovan Pulitzer [REDACTED]

[REDACTED]

[REDACTED]

⁴² Doug Logan Deposition Tr: 112:15-20

⁴³ This entry is redacted in the PDF version but is unredacted in the text version.

⁴⁴ Dean Felicetti Deposition Tr: 296:6-18

⁴⁵ Ibid, Tr: 303:12-304:4

[REDACTED]

[REDACTED]

70. [REDACTED]

Todd Sanders, [REDACTED]

[REDACTED]

[REDACTED]

Logan testified that he later determined that “Cjames” was Conan James Hayes.⁴⁸

71. [REDACTED] Phil Waldron [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

72. [REDACTED]

Russ Ramsland from ASOG, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁴⁷ [REDACTED] 14, [REDACTED]

⁴⁸ Exhibit 14, [REDACTED]

⁴⁹ Doug Logan Deposition Tr:139:17-23

⁵⁰ Exhibit 14, [REDACTED]

⁵⁰ Ibid, p. 12

“ [REDACTED]

[REDACTED]⁵¹

73. The available evidence did not indicate whether any Coffee County election software or data was given to Waldron, Bundren, or Ramsland.

74. At least until recently, Logan possessed the Coffee County election software and data collected by SullivanStrickler. He produced copies on a hard drive under subpoena for this case.

75. Thus, evidence shows that six individuals, affiliated with at least five organizations, downloaded Coffee County election software and data from SullivanStrickler’s ShareFile account during January 10 through February 25, 2021: Doug Logan, Todd Sanders, Conan Hayes, James Penrose, Michal Pospieszalski, and Jovan Pulitzer. Evidence suggests it may have been distributed further by some of those individuals.

Distribution via FedEx in April 2021

76. [REDACTED] Jeffrey Lenberg [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁵¹ Ibid, p. 8

[REDACTED] Lenberg testified that he does not recall downloading data from SullivanStrickler's ShareFile.⁵³

77. Two days later, on April 22, 2021, James Penrose emailed Paul Maggio and copied Stefanie Lambert, an attorney, and Greg Freemyer. The subject was: "Coffee County Forensics FEDEX Request". Penrose wrote, "Can you please FEDEX all the forensics material from the Coffee County acquisition to the same address as before. Please include the VMs on your download site as well." He continued, "Invoice Stefanie Lambert for the work like last time." Maggio replied to Penrose's email with, "This is received and we will begin the process of copying everything to a drive."⁵⁴

78. In the evening on the following Tuesday, Maggio emailed a co-worker, attached a FedEx label, and asked her to "please get this out tonight."⁵⁵ The FedEx label is for an overnight delivery on April 27, 2021 from the office of SullivanStrickler in Forest Park, Georgia to Stefanie Lambert at an address in Royal Oak, Michigan.⁵⁶

⁵² Exhibit 14, p. 9

⁵³ Jeffrey Lenberg deposition, 177:14-19

⁵⁴ Exhibit 15, Penrose-Maggio email re: Hard Drive to Lambert

⁵⁵ Exhibit 16, Maggio email to send FedEx

⁵⁶ Exhibit 17, FedEx label

79. The address in Royal Oak, Michigan is associated with Michael Lynch,⁵⁷ a private investigator.⁵⁸ Lenberg testified, “Michael Lynch worked with Stephanie Lambert. I believe he’s kind of a private investigator, that even before the elections was working with Stephanie Lambert. And once Stephanie got involved in the election stuff, I believe Lynch was kind of her right-hand man [...]”⁵⁹

80. On April 28, 2021 at 7:55pm, Lambert forwarded Maggio’s emails about the FedEx shipment and the password needed to access the encrypted hard drive to Lenberg, and he responded “Got it.”⁶⁰

81. Lenberg testified, “[A] disk drive from SullivanStrickler requested by Penrose and Stephanie Lambert was being sent to Michigan, and that disk went to Michael Lynch. Michael Lynch brought it over to the location I was at. I had a safe for safekeeping of any items. It was put in the safe. At some time, they asked me to make a copy of that, which they—I do not know what they did with it. It was provided to them to do something with it, but I was directed by Lambert and Lynch to make a copy. And then Michael Lynch retrieved the—that disk that was sent. And he took it for safekeeping somewhere else. [...] I was not involved in the

⁵⁷ VoterRecords.com website, <https://voterrecords.com/voter/86706878/michael-lynch>

⁵⁸ Michigan Council of Professional Investigators Directory, p. 7
<https://mcpihome.com/directory.php?p=7>

⁵⁹ Jeffrey Lenberg Deposition Tr: 103:9-16

⁶⁰ Exhibit 18, Lenberg-Lambert email, p. 9

[email] chain until the very end because they wanted me to make a copy, which they were going to do something else with. They sent me the password to be able to unlock it because it was encrypted.”⁶¹

82. The following Monday, May 3, 2021, Jeffrey Lenberg performed a demonstration with a Dominion EMS and ICP scanner/tabulator at Lynch’s Royal Oak address for a cable news channel video.⁶² Lenberg testified that the EMS software he used in the video was from Antrim County, Michigan—not Coffee County, Georgia, that the ICP he used was provided by Lynch and Lambert from “Michigan somewhere”, and that Lambert told him it was “lawfully obtained”.⁶³

83. Thus, evidence shows that three individuals, affiliated with at least two organizations, received Coffee County election software and data via Fedex in April 2021: Stefanie Lambert, Michael Lynch, Jeffrey Lenberg. In addition, Lambert and Lynch obtained a second copy for an unknown purpose.

Distribution via ShareFile in June 2021

84. Ben Cotton, from the company CyFIR, wrote in an affidavit in the District Court of Arizona, “In the course of my duties I have forensically examined

⁶¹ Jeffrey Lenberg Deposition Tr: 101:7-102:20

⁶² One America News Network, video via YouTube, May 3, 2021.
<https://www.youtube.com/watch?v=mX4KbcGt-Us>

⁶³ Jeffrey Lenberg Deposition Tr:153:3-155:1

Dominion Democracy Suite voting systems in [...] Coffee County Georgia, [...].”⁶⁴

85. CyFir and Cotton were engaged to review Georgia’s election software and data by the Law Office of Stefanie L. Lambert, PLLC. The engagement letter, dated July 3, 2021 and signed by Cotton and Lambert, lists “Forensic analysis of evidence” and “Expert reports and testimony”, and describes the evidence as “evidence obtained by SullivanStrickler from Coffee County, Georgia”.⁶⁵

86. By July 2021, Lambert had received the Coffee County election software and data from SullivanStrickler via FedEx, and Lenberg had made a second copy of it. Cotton was not given either of those copies.

87. Cotton testified at his deposition that James Penrose provided his credentials to enable Cotton to access SullivanStrickler’s ShareFile account, and—while logged in as Penrose—Cotton downloaded the Coffee County election software and data around June 11-12, 2021. Cotton testified that the data exists on a computer at his home in Montana on the day of his deposition.⁶⁶

⁶⁴ Declaration of Benjamin R. Cotton, *Lake v. Hobbs*, United States District Court for the District of Arizona, Case No. 2:22-cv-00677-JJT. June 8, 2022, <https://coalitionforgoodgovernance.sharefile.com/d-s26e084cef97f46d0b2147ec85d38f681>

⁶⁵ Exhibit 19, Cotton-Lambert Engagement Letter

⁶⁶ Benjamin Cotton Deposition Tr: 88:9-89:8 and 130:9-11

88. Thus, evidence shows at least one person, from another organization, received Coffee County election software and data from SullivanStrickler's ShareFile account during June 2021: Ben Cotton from CyFir.

89. For this portion of my analysis I concluded:

Coffee County election software and data was distributed to at least ten individuals between January and June 2021: Doug Logan, Todd Sanders, Conan Hayes, James Penrose, Michal Pospieszalski, Jovan Pulitzer, Stefanie Lambert, Michael Lynch, Jeffrey Lenberg, Ben Cotton. These individuals are affiliated with at least seven different organizations: #FightBack, CyberNinjas, Allied Security Operations Group, Defending the Republic, Mehow Consulting, Law Office of Stefanie L. Lambert, CyFir. Evidence suggests it was distributed further by some of those individuals.

V. Activity Related to Access on January 18-19, 2021

90. [REDACTED] James Penrose [REDACTED]

[REDACTED] Penrose, Misty Hampton (Coffee County Election Director), Doug Logan, and Jeffrey Lenberg. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁶⁷ Exhibit 14, [REDACTED]

91. Lenberg testified that the purpose of their trip to Coffee County was, “[W]e got notice, Penrose did, that another major anomaly had occurred during the runoff in Coffee County. And that in particular was that it appeared that the machine, the ImageCast Central [...] had been remotely reconfigured by Dominion apparently.”⁶⁸

92. [REDACTED] Lenberg [REDACTED]

[REDACTED]

[REDACTED]⁶⁹

93. [REDACTED]

[REDACTED] Lenberg, who resides in New Mexico, drove from Jacksonville, Florida. Logan drove from Sarasota, Florida.

94. Monday, January 18, 2021 was a holiday and the Election Office was closed. Security camera video shows Hampton, Logan, and Lenberg met at the Election Office at 4:20pm and Hampton’s daughter, DyAnna Hayes, joined them an hour later.

95. The security camera video provides few facts about their visit. The group spent most of their time in Hampton’s office, out of the view of the security camera. At 5:25pm, Hayes retrieved blank ballots from the storage room. At

⁶⁸ Jeffrey Lenberg Deposition Tr: 44:7-13

⁶⁹ Exhibit 14, [REDACTED]

⁷⁰ Exhibit 14, [REDACTED]

6:12pm, Hampton retrieved an ICP scanner from the storage room. Everyone left the Election Office at 8:06pm.

96. The following day, January 19 at 8:52am, Hampton, Logan, and Lenberg arrived at the Election Office. They spent most of their time in Hampton's office. At 10:58am, DyAnna Hayes arrived. At 1:20pm, Hayes retrieved a second ICP scanner from the storage room. At 6:02pm, Hayes retrieved a roll of paper tape for printing ICP election results. The group left the Election Office at 6:19pm.

97. Evidence indicates Eric Chaney, an Election Board member, was aware of their visit. On January 19 at 10:35am, Hampton texted Chaney "If you happen to be in town, the guys measuring my desk are still here".⁷¹ "Measuring my desk" appears to be a code phrase between Chaney and Hampton. She would use it again in a text to Chaney on January 27. Hampton testified that the phrase was indeed a reference to Logan and Lenberg, but pled the Fifth Amendment when asked why she used it and when asked if she thought there was something wrong with what they were doing.⁷²

98. Lenberg testified about their activities: "[For ICP testing] Misty got on her BMD, an ICX that she had there, and she created a number of ballots [...] [Misty] got out, I believe, 40 blank ballots that were left over from the 2020

⁷¹ Exhibit 20, Hampton-Chaney Messages re: measuring the desk

⁷² Misty Hampton Deposition Tr: 124:5-125:14

election, and we helped fill out those ballots by hand. And those were the ballots that were used to test the ICC. [...] [DyAnna Hayes] ran the ICP, while Doug observed that, and Misty Hampton ran the ICC, while I observed that. And we basically ran lots. When you do testing like this, you've got to get statistics right, so you run batch after batch after batch. And we were running the same ballots over and over and over and over".⁷³

99. To better understand Logan and Lenberg's activities while in the Election Office, I reviewed forensic images made from the Coffee County EMS and ICC computers more than 18 months after their activity in January 2021.

100. I was given a hard drive containing the forensic images for the Coffee County EMS and ICC made by a contractor for the State Defendants, Jim Persinger of PM Investigations ("PMI Hard Drive"), and a hard drive containing forensic images for the EMS and ICC made by a contractor for the Plaintiffs, Relevant Data Technologies ("RDT Hard Drive").

101. Metadata for the forensic images on both hard drives shows that they were made from the same physical hard drives as the EMS and ICC forensic images found on the SSA Hard Drive. Metadata on the PMI Hard Drive shows a forensic image was created from the EMS on July 5, 2022 and from the ICC on September 15, 2022. Metadata on the RDT Hard Drive shows a forensic images

⁷³ Jeffrey Lenberg Deposition Tr: 110:22-112:5

was created from the ICC on September 16, 2022 and from the EMS on September 22, 2022.

102. These forensic images are imperfect evidence. State Defendants represented that the EMS and ICC were removed from Coffee County on June 8, 2021 but have not produced any chain of custody evidence dated prior to July 2022. Chain of custody evidence begins on July 1, 2022 when Persinger took possession of Coffee County's EMS and ICC from Michael Barnes.⁷⁴ I cannot assess with certainty what changes may have been made before that date, and Persinger makes a similar statement in his declaration.⁷⁵

103. Once in his custody and after he made the forensic image of the EMS, Persinger made modifications to the original computer, in part by resetting the primary user's password.⁷⁶ These actions modified evidence that would allow independent verification that his copy is an accurate copy of the original. Additionally, Persinger waited for over two months to make the forensic image of the ICC. I must rely on Persinger's representation that no other changes were made while the servers were in his custody.⁷⁷

104. I created virtual machines from the forensic images on the PMI Hard Drive and RDT Hard Drive. I reviewed the system and application log files. I

⁷⁴ Exhibit 21, Declaration of James Persinger (Nov. 10, 2022), Exhibit C - Chain of Custody

⁷⁵ Exhibit 22, Declaration of James Persinger (Nov. 10, 2022), ¶ 17.

⁷⁶ Exhibit 22, Persinger Declaration, ¶ 23.

⁷⁷ Ibid, ¶ 51.

compared data to the forensic images on the SSA Hard Drive to understand what activity occurred in the intervening months. I consulted with Dr. Alex Halderman who also reviewed the hard drives for the Curling Plaintiffs.

105. A review of these forensic images revealed an important detail. On January 19, 2021 at 10:42am and at 10:47am, the system date on the ICC and EMS were changed to November 5, 2020 (75 days earlier) and were never restored to the true date.⁷⁸

106. Lenberg testified that he suggested changing the system dates because, if there was malicious code installed, “one of the things that a bad actor would do potentially is use the date as a trigger.”⁷⁹ When asked why he did not change it to November 3, the date of the 2020 General Election, Lenberg testified, “I don’t remember the exact reason why other than I was trying to do something close to the election, but not the election, to make sure I was in what might be a window in which a subversion was [...] triggered [...] so that they could defeat logic and accuracy testing and survive a machine recount.”⁸⁰

107. The practical result of the system date change was that EMS and ICC began using the modified date when logging events and creating and modifying

⁷⁸ Exhibit 23, Windows event logs, p. 1-2

⁷⁹ Jeffrey Lenberg Deposition Tr: 117:7-9

⁸⁰ Deposition of Jeffery Lenberg Tr: 120:7-9

files. For clarity of reading, I will reference the true dates, which requires adding 75 days to the dates in the evidence.⁸¹

108. The data for the ICC contains a file, “slog.txt”, which is used by the Dominion software to log information about user activities.⁸² On January 18, the log file shows that the ICC scanned 772 ballots in 6 batches. On January 19, the log file shows that the ICC scanned 5,084 ballots in 33 batches. In the final 11 batches, beginning at 5:11pm, the log file recorded a noticeable increase in scanner errors and batches that halted on ambiguous marks on a ballot.

109. Lenberg testified that, at around this time, he looked through Coffee County’s copy of the ICC software manual and discovered that “built into the Dominion software is an interface to tweak the scanner settings [...] And so what I did is I asked Misty to start changing those parameters to see if they made any difference.”⁸³ Lenberg produced hand-written notes dated January 19 which document changes to each of these parameters, including brightness, contrast, gamma, moire reduction, color drop-out, skew, and double feed detection.

110. There is less evidence about their use of the two ICP scanners that were brought into Hampton’s office during their visit. The evidence does not

⁸¹ The log files require meticulous examination because, not only do some dates require adjustment, the computers logged events more than once for dates in the November 2020 to January 2021 time period.

⁸² \DVS\Training Absentee By Mail ICC\Project\1_08_150_0_slog.txt

⁸³ Jeffrey Lenberg Deposition Tr: 124:9-126:10

include forensic images of that data. The ICPs were used in subsequent elections and their CompactFlash cards were likely re-used and overwritten.

111. Logan's testimony suggests the system date on the ICP was set to an earlier date, as was done on the EMS and ICC. "[Y]ou put the date to that time period of what it was on election day, and then you know that if any sorts of triggers it could have been in place are likely also to trigger again, and you would see the – the resulting behavior. [...] [W]hen you boot up the ICP device, I believe one of the things that displays when you check and validate, when you start an election is date and time."⁸⁴

112. I reviewed a report authored by Logan which states that scans were performed on 677 test ballots in an effort to determine whether the ICP showed bias against ballots marked for Donald Trump.

113. Lenberg testified that they also took the extraordinary step of opening up one of the two ICPs to scrutinize the parts inside. "[Misty] had a ICP that was being sent back for repair. And she – because she wanted to know whether or not there was remote access, she took the cover off [...] and let us look inside to see whether or not there was a modem inside the equipment. [...] We found a slot that – where you could add in a card that was near the outside. It appeared that it could

⁸⁴ Doug Logan Deposition Tr: 4:25-43:9

have been a modem add-in, there's no guarantee, but we did not see anything that appeared to [be] a modem to us inside.”⁸⁵

114. On January 20, 2021, the day after Logan and Lenberg departed Coffee County, [REDACTED]

[REDACTED] Penrose, Logan, and Lenberg. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

115. [REDACTED] Lenberg [REDACTED]

[REDACTED]

[REDACTED]

116. For this portion of my analysis I concluded:

During January 18-19, 2021, Doug Logan and Jeffrey Lenberg were given extraordinary access to Georgia's voting system in Coffee County by the Election Director, Misty Hampton. They had access for over 13 hours,

⁸⁵ Jeffrey Lenberg Deposition Tr: 289:13-290:16

⁸⁶ Exhibit 14, [REDACTED]

⁸⁷ Ibid, p. [REDACTED]

including hours when the Election Office was closed to the public. During their visit, the system dates on the election computers were changed, scanner settings were reconfigured several times, over 6,500 ballots were scanned, and one precinct scanner was opened up to inspect the parts inside. Their work was organized by James Penrose and Charles Bundren.

VI. Activity Related to Access on January 25-29, 2021

117. [REDACTED]

[REDACTED] Jams Penrose, Doug Logan, and Jeffrey Lenberg, [REDACTED]

118. Security camera video shows that Lenberg arrived at the Coffee County Election Office on January 25 at 1:18pm. He spent most of the time in Misty Hampton's office with Hampton and her daughter, DyAnna Hayes, out of the view of the security camera. At 1:49pm, Hayes retrieved an ICP and blank ballots from the storage room. At 2:23pm, Hampton retrieves an ICX ballot marking device and

⁸⁸ Exhibit 14, [REDACTED]

printer. At 4:00pm, Hampton retrieves blank ballots from the storage room. At 5:33pm, Lenberg leaves the Election Office.

119. A review of the forensic images on the PMI Hard Drive and RDT Hard Drive provided more evidence of their activities inside the office. I was cognizant that the system dates on the EMS and ICC had been modified (and they would be modified again). For clarity of reading, I will reference the true dates, which at the outset requires adding 75 days to the dates in the evidence.

120. The Dominion Election Event Designer software (EED) installed on the EMS records user activity in a log file. The log shows that, on January 25 between 2:20pm and 2:42pm, EED was used to program a CompactFlash for use with an ICP scanner and to program a USB drive and Smart Card for use with an ICX ballot marking device.⁸⁹

121. The Windows event logs show that the system date and time on the ICC was changed twice more on January 25. At 4:25pm, it was set to November 3, 2020 at 8:25am (83 days and 8 hours before the true time). At 5:01pm, it was set to November 5, 2020 at 9:01am (81 days and 8 hours before the true time).⁹⁰ It was never changed back to the true time. The EMS date and time was not changed further; it remained 75 days behind the true time.

⁸⁹ “\Program Files\Dominion Voting System\Log\Info.log”

⁹⁰ Exhibit 23, Windows event logs, p. 3-4

122. Lenberg produced hand-written notes dated January 25 which document scanning batches of ballots “hand filled by Jeff” and “Misty made (all QR)”. The ICC log file, “slog.txt”, shows that 559 ballots were scanned in 25 batches on January 25, 2021. The last ballot was scanned at 5:26pm, four minutes before Lenberg left the Election Office for the day. It was also the last ballot scanned during the week.

123. On the second day, January 26, 2021, security camera video shows Lenberg arrived at the Election Office at 10:30am and went into Hampton’s office. At 11:08am, an Inspector with the Georgia Secretary of State Investigations Division arrived at the Election Office to speak with Hampton. Lenberg exited Hampton’s office and went into another room while the Inspector and Hampton met in Hampton’s office. After the Inspector left, Lenberg returned to the main room and looked out the window—an action that appears to be making sure the Inspector had left. Soon after, at 11:15am and only seven minutes after the Inspector’s arrival, Lenberg departed the Election Office.

124. Evidence indicates Election Board member Eric Chaney was aware of Lenberg’s follow-up visit that week. The following morning, January 27 at 9:23am, Hampton texted Chaney, “I took care of the people measuring my desk”,

again using the same code phrase used on January 19 to reference Lenberg's activities.⁹¹

125. On the same day, soon after that text, security camera video shows Lenberg arrived at the Election Office at 9:59am, went into Hampton's office, and departed at 10:22am, after only 23 minutes had elapsed.

126. [REDACTED] Lenberg [REDACTED] Penrose and Logan [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

127. The same day, at 9:12pm, Lenberg submitted an Open Records Request ("ORR") to Coffee County. Lenberg wrote that he was "doing independent research to help verify the accuracy of the 2020 General Election." He requested copies of the ICP results tapes and the batch and tally sheets for the "full hand recount" of the 2020 General Election. His request stated that he would provide a thumb drive to accept the records.⁹³

⁹¹ Exhibit 20, Hampton Chaney Messages re: measuring the desk

⁹² Exhibit 14, [REDACTED]

⁹³ Exhibit 24, Lenberg Open Records Request, p. 3

128. On the fourth day, January 28, 2021, security camera video shows Lenberg arrived at the Election Office at 2:11pm, went into Hampton's office, and left again at 2:21pm, after only 10 minutes had elapsed.

129. Lenberg produced a compressed file in the Zip format, named "Coffee CF.zip", which he represented he received from Hampton via a thumb drive on or around January 28, 2021. The file was password protected to prevent decompression to reveal its contents. Lenberg testified that he did not know the password, and he was unable to locate it.⁹⁴

130. I was able to determine the correct password for the file using other information in the evidence. When unlocked and decompressed, it yields a directory containing 18 subdirectories, named "CF01" through "CF18". The subdirectories contain data from the 2021 Run-off Election, copied from the 18 CompactFlash cards used in Coffee County's ICPs. They are not forensic images of the cards, like those created by SullivanStrickler. Instead, the data includes only the visible files from each card: scanner configuration files, election results, log files. The ballot images, which would not be readily visible to a user examining a CompactFlash card, are not included. The file metadata shows that the directories holding the data were created on January 27 between 2:50pm and 2:56pm.

⁹⁴ Jeffrey Lenberg Deposition Tr. 184:17-185:1 and 330:4

131. These files do not fit the description of the records Lenberg requested in the ORR. Lenberg testified that he did not believe these files were intended to be a response to the ORR, that he requested them from Hampton independently.⁹⁵ However, on February 4, 2021, Hampton emailed the records administrator that Lenberg's ORR was complete and could be closed. Hampton wrote, "He gave me a thumb drive and I put it on the thumb drive," and "The information on the thumb drive was a copy of the top part of the ICP tape, the batch sheets from the hand recount and the tally sheet from the hand recount".⁹⁶ The evidence does not include any additional files that match the ORR.

132. On the fifth and final day of Lenberg's visit, security camera video shows that Lenberg arrived at the Election Office at 2:33pm. He spent most of the time in Hampton's office. At 3:27pm, Lenberg and Hampton retrieved a KNOWiNK Poll Pad. He departed at 3:57pm.

133. Lenberg testified about using the Poll Pad, "I believe they actually demonstrated to me the pollbook. But other than telling me how it worked, demonstrating it, they showed me that [...] it was connected to the internet during its operation and that they literally could go order Domino's Pizza and have it delivered while it was connected to the internet."⁹⁷

⁹⁵ Jeffrey Lenberg Deposition Tr: 188:2-15

⁹⁶ Exhibit 25, Hampton-Vickers email re: ORR

⁹⁷ Jeffrey Lenberg Deposition Tr. 71:21-72:7

134. For this portion of my analysis I concluded:

During January 25-29, Jeffrey Lenberg was again given extraordinary access to Georgia's voting system in Coffee County by the Election Director, Misty Hampton. He had access for almost seven hours over five days, and he had intended to have significantly more. During his visit, the system date on the central vote tabulator was changed twice (and never changed back), media was created to program a precinct scanner and a ballot marking device, 559 ballots were scanned, and he was given voting system data to take with him.

VII. Authorization

135. A foundational issue before assessing the implications of these activities is determining what authorization had been given for them and by whom. Authorization is distinct from whether these activities were legal—I am not a lawyer and offer no opinion on legality. Unauthorized activity implicates failures in oversight, processes, or controls, which are significant for assessing security.

136. My experience is that only explicitly authorized individuals are permitted to access a voting system, and the authorizations are typically enumerated in state law or in the election software vendor in a license agreement with the jurisdiction. Authorization for other parties to access a voting system is

exceedingly rare and, when granted, is usually by order of a court and for a clear purpose.

137. The level of access to Georgia's voting system in this case was extraordinary. The voting system components were accessed, analyzed, tested, and manipulated by many individuals, often with little oversight. Most of the voting system software was duplicated and distributed widely to many individuals, with many affiliations, most of whom reside outside the state of Georgia. It is notable that the purpose of allowing such extraordinary access remains murky. Various reasons were given during depositions, but the reasons do not align. So, who authorized such breadth and depth of access?

138. I saw no evidence that any court authorized these activities or even any evidence of any active litigation related to them.

139. The Secretary of State's office has represented that they did not know about these activities, and therefore could not have authorized them. In addition, on November 17, 2020, Elections Divisions Director Chris Harvey sent an Official Election Bulletin to all Georgia counties explicitly advising that no third party should be given election software and data.⁹⁸

140. Dominion Voting Systems is unlikely to have given authorization, because several months later, on May 6, 2021, they sent a Customer Notification to

⁹⁸ Exhibit 26, Chris Harvey Official Election Bulletin

all Georgia counties which stated, “It is critically important that only authorized, legal users be granted access to voting equipment in order to maintain secure chain of custody for your system” and that the software license states “who can legally access the system with the company’s consent” but “does not allow for the release of voting systems to unaccredited, non-certified third parties without prior written consent.”⁹⁹

141. SullivanStrickler initially received a text from “Katherine” who cited a “written invitation” from Coffee County. SullivanStrickler testified that they believed the work was authorized by Coffee County election officials who were on-site and “[t]hat the direction provided [to] us was was under a legal umbrella of a directing attorney.” They testified that Sidney Powell, an attorney, was their customer, and they did not conduct due diligence on her representations of authorization in the engagement letter.¹⁰⁰

142. Doug Logan testified that James Penrose, who worked with Sidney Powell, told him it had been cleared by an attorney, but it was not Powell, “I even asked who the attorney was. And he told me it was Charles Bundren.”¹⁰¹ Logan continued, “I believe I talked with an attorney. Attorneys usually aren’t into breaking the law, that’s just not their thing, you know. [...] Going to a place,

⁹⁹ Exhibit 27, Dominion Voting Systems Customer Notification

¹⁰⁰ Dean Felicetti Deposition Tr: 71:3-73:9 and 75:3-16

¹⁰¹ Doug Logan Deposition Tr: 21:12-14

there's elected people there. You know, they know that we're coming, we're welcomed. I mean, what reason would I ever have to suspect that it wasn't authorized."¹⁰² However, Logan could not recall who Bundren's client was and stated, "It would be my assumption, but this is speculation, that it was the county itself."¹⁰³

143. Jeffrey Lenberg did not share Logan's view, despite the fact that they were working together. Lenberg testified, "I still don't know who Charles Bundren is."¹⁰⁴ Instead, he testified, "[M]y understanding is that Ms. Hampton was the election supervisor for the county and that she had full authority [...]"¹⁰⁵ Regarding the CompactFlash card data Lenberg obtained the following week, he testified, "I got a copy directly from the election supervisor, who I believe was authorized to give it to me,"¹⁰⁶ and that he was not working for any attorney when he obtained them.¹⁰⁷ Regarding the copy Lenberg made of the Coffee County software and data while in Michigan, he cited the direction of Stefanie Lambert, an attorney in Michigan.¹⁰⁸

¹⁰² Doug Logan Deposition Tr: 60:14-24

¹⁰³ Doug Logan Deposition Tr: 38:11-18

¹⁰⁴ Jeffrey Lenberg Deposition Tr: 77:14-15

¹⁰⁵ Jeffrey Lenberg Deposition Tr: 91:2-4

¹⁰⁶ Jeffrey Lenberg Deposition Tr: 202:17-19

¹⁰⁷ Jeffrey Lenberg Deposition Tr: 189:17-20

¹⁰⁸ Jeffrey Lenberg Deposition Tr: 101:17-18

144. When Misty Hampton was asked if “Eric Chaney told you in effect that these board members want you to allow someone to come in and copy the election software”,¹⁰⁹ and “was your understanding that the direction from Mr. Chaney extended from the access that was given on the 7th to additional access that was given on the 17th and the 18th”, she responded affirmatively to both questions.¹¹⁰ Hampton testified, “I didn’t do anything without the direction of Eric Chaney.”¹¹¹

145. The Coffee County Board of Elections testified that it did not know about or authorize these activities. In a deposition, a representative for the Board answered a series of questions:¹¹²

Q: Did the Board approve any of the individuals coming in on January 7, 2021, to be in the office and do any of the work they did there?

A: The Board did not approve that.

Q: Do you know whether Eric Chaney approved that on behalf of the Board or as a member of the Board?

A: I do not know if Eric Chaney approved of that. I will say any decision made requires a quorum of the Board.

¹⁰⁹ Misty Hampton Deposition Tr: 65:14-67:1

¹¹⁰ Misty Hampton Deposition Tr: 114:11-21

¹¹¹ Misty Hampton Deposition Tr: 120:7-8

¹¹² Coffee County Board of Elections Deposition Tr: 48:20-49:14

Q: So Mr. Chaney would not have the authority on his own to approve that work?

A: No.

Q: And as you sit here, the Board does not have any insight or understanding as to why Mr. Chaney was here for that work that occurred?

A: The Board does not.

146. Eric Chaney, now a former member of the Coffee County Board of Elections, pled the Fifth Amendment when asked about his involvement.

147. For this portion of my analysis I concluded:

Legitimate authorization was *not given* for the irregular access to Coffee County's Election Office in January 2021. The evidence indicates an illusion of authorization was created (1) by Eric Chaney leveraging his membership on the Board of Elections, (2) by Misty Hampton's willingness to collaborate, (3) by several attorneys—including Powell, Bundren, and Lambert—lending their integrity as officers of the court, and (4) by involving many other willing and credulous participants.

VIII. Implications

148. The focus of this portion of the analysis was to assess the implications of the information and events presented in the evidence, especially how they may impact the future security of elections in Coffee County and throughout Georgia.

149. In this portion, I depart from the documents and rely on the totality of my knowledge and experience regarding voting technology and cybersecurity.

150. Any analysis of the implications must begin by acknowledging that elections are national critical infrastructure. Election systems must meet a higher standard for security, reliability, and resilience than standard industrial and commercial systems. I also expect election systems to draw more attention from adversaries around the world than most systems do. Unlike other critical infrastructure, elections are the very foundation of our democracy. The health of our democracy depends on reliable elections with trustworthy outcomes. Any implications are magnified when viewed through that lens.

151. The scope of the access and data collection in Coffee County is broad and impressive. SullivanStrickler copied software and data from almost every component of Georgia's election system. It contains protected software and data that is unavailable by any other means to the public or even to election experts. The significance of its collection onto a single hard drive in the possession of someone outside an election office, followed by its unregulated distribution to

many others, cannot be overstated. These events were by any measure a consequential breach of Georgia's election security.

152. Below, I explain several implications in greater detail.

Insider Threats

153. If unauthorized individuals took unauthorized actions with election hardware and software, the most obvious implication is that the existing oversight, procedures, and access controls failed to prevent it. Unauthorized actions can be facilitated by someone with *authorized* access and credentials (an “insider”), such as an election board member, the election director, or others working in the election office.

154. Insider threats are a common security challenge but access can be more effectively regulated by various means. For example, a secure door can have multiple locks with keys held by different people. Another common defense to protect software and data from copying or alteration is to encrypt the hard drives and other storage media, which information security professionals generally refer to as “data at rest”. The encrypted data at rest can be copied, but it cannot be accessed without first decrypting it. Microsoft Windows—the operating system on the Coffee County EMS and ICC computers—has BitLocker software built-in which could encrypt the hard drives. BitLocker encrypted data can only be accessed by using a password hidden in the computer's hardware or by using a

secret “recovery” password. BitLocker is not used by Georgia’s voting system. If it had been used, it would have made it difficult to make forensic images of those devices, even with insider assistance.

155. Insiders facilitated the activities in Coffee County in January 2021 and the oversight and access controls to protect election hardware and software were insufficient.

Implications for Coffee County’s Election Hardware

156. Any time election hardware is accessed without authorization or its chain of custody is broken, it introduces a significant risk the hardware has been manipulated or damaged—intentionally or inadvertently—and the flaws will not be detected or remediated. Afterwards, the hardware should be considered unreliable and untrustworthy.

157. One cannot know whether manipulation or damage occurred in the course of the data acquisition in Coffee County. The systems could be tested exhaustively, pass all tests, and yet still fail to find a problem. It is difficult to prove a negative. The documents show there was ample access and opportunity for manipulation or damage.

158. There are several examples during Doug Logan and Jeffrey Lenberg’s visit. Lenberg directed much of the work, yet he testified that it was his first

experience with a voting system’s “hands-on equipment”.¹¹³ The protective case of an ICP scanner was opened up to reveal its sensitive interior parts. Several computer configurations were modified but never restored. These actions were abnormal and reckless. They could easily have created problems that would prevent the system from functioning or from accurately recording votes in an election. Lenberg’s own tests demonstrate that some scanner settings can prevent ballots from scanning properly.

159. Another example is that the photographs produced by SullivanStrickler show Coffee County election hardware connected to unauthorized devices—a UEFI USB drive and external hard drive—and running unauthorized software. SullivanStrickler’s devices and software are uncertified and untested for use with Georgia’s election hardware and software. They may have flaws or incompatibilities that cause damage.

160. The risk of contamination increases if SullivanStrickler’s devices and software were used in other digital forensic work, where malware may be encountered frequently. It is my understanding that SullivanStrickler performs digital forensic work routinely for a variety of clients. And, as noted earlier, a write-blocker was not used during the data acquisition to prevent mistakes by the technician or transmission of malware.

¹¹³ Jeffrey Lenberg Deposition Tr: 17:1-7

161. There are second-order effects to consider as well. If hardware with a broken chain of custody is ever connected to a network, other hardware, or removal media, there is a risk that malware present on the device will spread to other devices, and then from those devices to other devices, like a contagion. The EMS acts as a hub. The EMS puts data on removable media (CompactFlash cards, USB drives) which is installed in scanner/tabulators (ICPs) and the ballot marking devices (ICXs) before the election. After the election, that removable media comes back to the EMS so that it can extract data and reprogram them for the next election. The EMS is also connected via a local-area network (LAN) to the ICC scanner/tabulator so that data can be exchanged both ways easily. All of these devices are interconnected. Every use is a new opportunity for contagious transmission of malware between them.

162. The risk of contagious transmission increases when removable media is reused. The evidence shows that Coffee County reuses removable media for several elections, such as the CompactFlash cards used with ICP scanner/tabulators. Reuse of removable media is a bad security practice because it provides a convenient vehicle for malware to move between devices in both directions—from the EMS to other devices, and from devices back to the EMS. It is analogous to intravenous drug users sharing needles. The U.S. Election Assistance Commission (“EAC”) recommends using “single-use memory devices

to transfer election results from the voting system tabulator to the EMS” and “write-once or read-only removable media should be used, where possible”.¹¹⁴

163. Because of these concerns, it is common practice for election hardware accessed without authorization or with a broken chain of custody to be decommissioned and not used in future elections, and then quarantined and never connected to a network, other hardware, or removable media. When equipment chain of custody was broken recently as a result of similar incidents¹¹⁵ in Arizona, Pennsylvania, Colorado, and Michigan, the election hardware was quickly decommissioned by their Secretaries of State.

164. The Cybersecurity and Infrastructure Security Agency (“CISA”) recommends election officials address “Incident Eradication” by taking several steps: remove compromised machines, block known malicious infrastructure, reset account credentials, and implement additional controls.¹¹⁶ I strongly agree.

165. The State Defendants represented that the EMS and ICC were removed from Coffee County on June 8, 2021, though its removal was not attributed to unauthorized access. The remaining election hardware remained in service,

¹¹⁴ U.S. Election Assistance Commission, “Best Practices for Election Technology”, 19, https://www.eac.gov/sites/default/files/electionofficials/security/Best_Practices_for_Election_Technology_508.pdf

¹¹⁵ Many of the participants in Coffee County activities are implicated in these incidents too.

¹¹⁶ Department of Homeland Security, “Incident Handling Overview for Election Officials”, 5, https://www.cisa.gov/sites/default/files/publications/incident_handling_elections_final_508.pdf

through several elections, until it was replaced soon after September 23, 2022.¹¹⁷

Before that time, it was not quarantined and was connected to other hardware via removable media several times. The failure to immediately quarantine *all* affected hardware may have already resulted in the contamination of other devices, including the replacement EMS and ICC, which are still in use.

Implications of Distribution of Election Software

166. Unfortunately, control over the election software and data cannot be reestablished after the fact. The horse has left the barn.

167. The software and data were distributed widely in the first month and 23 months have passed since. No one can know how many copies exist around the world or who possesses them. Digital data is easy to duplicate, transmit, and conceal. Copies may have been traded or sold. Copies may be readily available online for public download.

168. Unregulated possession of the software and data carries an inherent risk of *further* distribution, both intentional and unintentional. Copies may be in the possession of parties who would willingly distribute them further or simply fail to keep them safeguarded. Every additional copy in circulation has the potential to compound all of the other negative effects. In other words, all risks are lower if

¹¹⁷ <https://sos.ga.gov/news/raffensperger-replace-coffee-county-election-equipment-end-distraction-local-election>

three adversaries obtain copies rather than four, which is still far better than 40 or 400.

169. Unauthorized copying and distribution of election software and data does not only impact Coffee County. All Georgia counties use the same software. And beyond Georgia, many other jurisdictions in the United States use similar software. They all share in the implications of its distribution.

Distribution Emboldens and Increases Adversaries

170. Most voting system vendors, including Dominion Voting Systems, strictly limit who may possess and review their proprietary software code. I am familiar with the terms and conditions in several vendor sales contracts. They grant customers a non-transferrable license to *use* the software and prohibit any duplication, sharing, or inspection of the software or its source code. Often, the state government will not even possess a copy of the source code; the vendor will place it in secure escrow instead.

171. Access to devices with election software installed is usually strictly controlled. The election office and storage areas keep sensitive equipment behind locked doors with few keys and may monitor them with cameras or personnel. Election hardware includes locks and tamper-evident seals to restrict access to their data storage. Together, these measures have made election software difficult to obtain without investing significant time and extensive resources.

172. Unfortunately, the Coffee County data breach and uncontrolled software distribution have significantly lowered the resources required for adversaries to obtain Georgia's election software and data. Obtaining the software today may be as easy as clicking a link. With slightly more effort, adversaries could bribe, rob, con, or otherwise persuade someone in possession of the software.

173. Greater availability of the software expands the landscape of potential threats. Voting system security experts like myself have historically considered the most dangerous potential adversaries to be large foreign nation states, who have extensive resources. However, the widespread distribution of the Dominion software greatly expands the universe of potential adversaries. It lowers the effort required for adversaries with extensive resources, and it creates *new* opportunities for adversaries with modest or even meager resources—from small nation states down to a person working alone in a basement. More adversaries increases the potential threats to election systems and increases the likelihood one will succeed in causing an incident.

Distribution Facilitates Disinformation

174. A highly likely consequence of the distribution of election software is that knowledge about its code and operation will be used in disinformation

campaigns. This is not theoretical. There are *many* recent examples to serve as warnings.

175. The most prominent example has to be the Allied Security Operations Group’s Antrim report (“ASOG Report”). The report was authored by ASOG’s Russell Ramsland on December 13, 2020 regarding the Dominion voting system in Antrim County, Michigan.¹¹⁸ Among its many findings, the ASOG Report concluded the voting system was “intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results.” Its most cited and incendiary claim was that ASOG examined the voting machine logs and found there was a 68% error rate.

176. Almost every finding in the ASOG Report was quickly debunked by experts, including the purported 68% error rate. On December 16, Chris Krebs, the former chief of CISA, testified to the Senate Homeland Security and Governmental Affairs Committee that the ASOG Report was “factually inaccurate” and debunked several of its claims.¹¹⁹ Dr. Alex Halderman wrote an analysis for the Michigan Secretary of State in which he refutes ASOG’s findings and explains how ASOG

¹¹⁸ The report was produced for *Bailey v. Antrim County*, Michigan Circuit Court for the County of Antrim, Case No. 20-9238-CZ, a case in which four SullivanStrickler employees, Conan Hayes, and Todd Sanders traveled to Antrim in December 2020 and made forensic copies of the EMS, CompactFlash cards, and USB drives, which were then analyzed by them and by Phil Waldron, Doug Logan, James Penrose, Ben Cotton, and Jeffrey Lenberg.

¹¹⁹ Chris Krebs, Testimony on “Examining Irregularities in the 2020 Election”, December 16, 2020. <https://www.rev.com/blog/transcripts/fired-election-official-chris-krebs-senate-testimony-on-2020-election-security-transcript>

egregiously misconstrued the logs by counting benign warnings, multiple attempts to scan a ballot, and other expected behaviors as “errors”. Normal system operation was presented as nefarious.

177. The ASOG Report made an impact anyways. Matt Masterson, senior advisor on elections at CISA, described its significance to *The Washington Post*:

Of all the ways in which Ramsland pushed the stolen-election narrative, arguably the most damaging was an ASOG report on Dominion machines in Michigan’s rural Antrim County, said Masterson, the senior cybersecurity adviser who was then focusing on elections at DHS. Repeatedly and at key moments, Masterson said, ASOG was the source of morsels of inaccurate information that shaped public perception. [...]

“It wasn’t just that the president would tweet about their stuff. It was all these little nuggets and grist that they provided or that were cited to them in testimony or in the ‘kraken’ cases. It provided the appearance of substance and fact to something that had no substance or fact,” said Masterson, [...] ¹²⁰

¹²⁰ Emma Brown, Aaron C. Davis, Jon Swaine, and Josh Dawsey, “The Making of a Myth”, *The Washington Post*, May 9, 2021. <https://www.washingtonpost.com/investigations/interactive/2021/trump-election-fraud-texas-businessman-ramsland-asog/>

178. On December 14, the same day the Michigan judge authorized its release, the ASOG Report made it all the way to the desk of President Trump, who forwarded it to Attorney General Barr for review. President Trump also tweeted about the report several times, saying it revealed massive fraud. The ASOG Report became the centerpiece of a December 16 draft Executive Order to seize all voting machines and to appoint a special counsel for a nation-wide fraud investigation.¹²¹ These measures are consistent with proposals contemplated by President Trump at a meeting in the Oval Office on December 18 with Michael Flynn, Sidney Powell, and others.¹²²

179. ASOG used their access to the election software, which the general public did not have, to misrepresent its features and its reliability in order to influence the outcome of an election which had already concluded. It is difficult to imagine how examining election software could result in more consequential disinformation than that which almost causes the seizure of voting machines and risks the peaceful transfer of power on which democracy depends.

¹²¹ Betsy Woodruff Swan, “Read the Never-Issued Trump Order That Would Have Seized Voting Machines”, *Politico*, January 21, 2022. <https://www.politico.com/news/2022/01/21/read-the-never-issued-trump-order-that-would-have-seized-voting-machines-527572>

¹²² Jonathan Swan and Zachary Basu, “Inside the Craziest Meeting of the Trump Presidency”, *Axios*, February 2, 2021, <https://www.axios.com/2021/02/02/trump-oval-office-meeting-sidney-powell>

Distribution Facilitates the Subversion of Election Software

180. A core cybersecurity principle, borrowed from the field of cryptography, is Kerckhoff’s principle: “One ought to design systems under the assumption that the enemy will immediately gain full familiarity with them.”¹²³ A popular and terser version is Shannon’s maxim: “The enemy knows the system.”¹²⁴

181. This is sound security advice for designing a cryptographic system, and it applies well to network, hardware, and software design. Its intent is to discourage over-reliance on obscurity as a security defense. If one builds a cipher device to assist the military in sending coded messages, one should build it with the expectation that another military will obtain one of the devices eventually and deconstruct it to learn its secrets.

182. It is tempting to apply Kerckhoff’s principle to the distribution of election software, to shrug our shoulders and reason that the “enemy” already had a copy of the “system” so little has changed. That would be a mistake. There is a big difference between good design advice and the *actual circumstance* of an adversary possessing the “system.” One can design a system for the *eventual* circumstance and also hope it arrives late. In the actual circumstance, years may pass before one adversary “knows the system,” and years more before the second

¹²³ Auguste Kerckhoffs von Nieuwenhof, “La Cryptographie militaire,” 1883.

¹²⁴ Attributed to cryptographer Claude Shannon.

and third do. Moreover, my experience has been that election software frequently fails to heed Kerckhoff's principle and overly relies on obscurity, physical protections, access controls, and procedures to guard its secrets. *If one failed to plan for the day the enemy eventually knows the system, then its secrets are quickly discovered when that day actually arrives.*

183. A country, organization, or person can develop techniques or code to subvert the software's intended operation. Possession of the software is *invaluable* to such a process. The software is more than just a blueprint. It is a functional copy that can run on standard, commercial hardware. The precise details of its operation can be closely inspected. An adversary can test theories and evaluate the results. An adversary can craft modifications to the software, verify they work, and then refine them to be more potent or less detectable. Any adversary with the software can build a hands-on engineering laboratory, or several.

184. For example, Doug Logan created several virtual machines from the forensic images and shared them with his collaborators. These are easy-to-use versions of Georgia's election software. Logan produced a screenshot in which the ICC software appears to be running in a virtual machine, and the computer is monitoring the processes (various tasks the software is doing) in one window, while another window runs a program called Immunity Debugger.¹²⁵ Immunity

¹²⁵ Exhibit 28, Screenshot, originally titled "drillingIn.png"

Debugger is described as “a powerful new way to write exploits, analyze malware, and reverse engineer binary files.”¹²⁶ In the screenshot, the dense letters and numbers on a black background show the actual software code as it is being run. The buttons above with symbols suggesting play, pause, and rewind are for controlling the operation of the software step-by-step. Logan testified, “The only thing that I ever recall using the debugger for was to try to figure out how they were handling encryption keys on the device.”¹²⁷ He also testified that he believes the encryption keys on the Dominion system are not well protected and “the encryption key that’s more than enough to change results on the [ICP scanner’s CompactFlash] cards”.¹²⁸

185. It is difficult to predict what subversions might result from such an analysis. The range of possibilities is large. It would depend on each adversary’s particular set of skills and resources, what their analysis discovered, and their goals and priorities.

186. Examples of potential subversion can be found in Dr. Alex Halderman’s July 2021 expert report, *Security Analysis of Georgia’s ImageCast X Ballot Marking Devices*.¹²⁹ Dr. Halderman and Dr. Springall approached their

¹²⁶ Immunity Debugger product website, <https://www.immunityinc.com/products/debugger/>

¹²⁷ Doug Logan Deposition Tr: 169:9-13

¹²⁸ Doug Logan Deposition Tr: 49:12-22

¹²⁹ Dr. J. Alex Halderman, *Security Analysis of Georgia’s ImageCast X Ballot Marking Devices*, 2021. (Sealed)

analysis of the vulnerabilities in the ICX in a similar fashion, but with *far less* software and data at their disposal than the software and data collected in Coffee County by SullivanStrickler. Over approximately 12 person-weeks, they identified multiple serious vulnerabilities and developed proof-of-concept attacks that could allow malware to subvert normal operation. These included attacks requiring minimal access to devices, and that could spread from device to device.

187. It would be naive to believe others are not capable of doing the same. The necessary skills are possessed by most nation states as well as hundreds of individuals around the world. The data collected by SullivanStrickler included the Android software that controls every ICX used in the State of Georgia, which is the very same software analyzed by Dr. Halderman and Dr. Springall. Today, the Coffee County election software has been out in the wild for 98 weeks, more than eight times as long as was used for their analysis.

188. A relatively easy subversion would be to prevent election systems from operating at all or from operating properly—a denial of service, slowing down the system, or other erratic behavior. It would not require much technical skill to cause damage. It could be as easy as deleting a file the system needs to operate. With basic skills, one might leverage code from one of many readily-available strains of ransomware that have become a common threat. The effect could be to create long lines or to prevent voters from casting votes. Preventing the reliable, orderly

conduct of elections could create stress and chaos, affect the election results, and would almost certainly diminish the public's trust in the voting system and in the election outcomes. Georgia's reliance on ballot marking devices to generate and print ballots greatly amplifies the impact such malfunctions would have on a polling place.

189. Given a forensic copy of a voting system component, and not merely the election software that runs on it, an adversary can analyze the election software in situ. An adversary can discover the various defenses and precise "hardening" measures that Dominion has taken to learn what is well protected and what is not. An adversary can develop techniques for hiding malware in out-of-the-way places to make it less detectable.

190. An adversary can identify vulnerabilities in the operating system or other libraries of code that can be exploited outside of the election software itself. Operating systems used in election components are not upgraded as frequently as in a typical office or home. Georgia's election software is Dominion Democracy Suite 5.5-A which was certified by the EAC in January 2019. Since then, there have been few updates (which Georgia does not use). There are few updates because, in part, the certification processes favor static, stable, well-tested systems over regular upgrades, bug fixes, and security patches which may have side effects that impact reliability. The downside of this approach is that older software often

has known vulnerabilities, which adversaries diligently catalog and stockpile, that remain unpatched and ripe for exploitation. The static nature of the software is a strength when well protected and a weakness when exposed to outsiders.

191. A moderately skilled adversary could reverse engineer the software. The election software is mostly compiled code which is efficient for computers to read, but not human readable. There are software programs designed to decompile and deobfuscate the code to make it human readable again. Then the code can be studied to understand which sections control which functions of the voting system. An adversary might rewrite sections of the code. They could add additional logic or remove protections and defenses. The code could be programmed to cheat or otherwise misbehave. Then the human-readable code could be recompiled for use by computers. The voting system software has features to help detect any changes to the code, but these features reside in the same software and could be reprogrammed at the same time.

192. Another target for subversion is the software's cryptography. Voting systems rely on cryptography extensively to validate the integrity and authenticity of software and data. They use cryptographic algorithms, which use cryptographic keys (not so different from passwords), to encrypt and decrypt data. If keys are kept private and secure, they can be used to digitally "sign" data to guarantee it comes from an authentic source and has not been altered since its signing.

193. A skilled adversary might discover how to subvert the cryptography in the system. Breaking cryptography directly is an unlikely, herculean task, but it is not uncommon to find weaknesses in the implementation of cryptography that offer fertile ground. The Georgia voting system software and data will indicate which cryptographic algorithms are being used and contain many cryptographic keys and other secret data. The EMS in particular holds many keys that it uses to encrypt and sign the data it provides to other devices, and to decrypt and validate the data they send back to it. The good news is that most of the keys are specific to a single election and will have no use or value in future elections. However, some keys or other secret data may be reused for every election, or studying the keys may reveal how they are generated and used. For example, if key creation incorporates the election name, date, or other knowable information an adversary could forge a key by using the same inputs. It is a bad practice, but one I do not rule out. In the worst case, the system may have a permanent, default password like “abcde”, as a popular but now out-of-use voting machine once did. One cannot predict whether the software’s use of cryptography is well designed and will withstand exposure.

194. Without cryptography, a voting system loses the ability to differentiate between legitimate, authorized data and fraudulent or harmful data. It becomes vulnerable to many attacks. An adversary can install different software or malware.

Edited or forged data can be accepted as legitimate. QR codes that store vote selections can be altered but appear valid. Vote totals, cast vote records, ballot images, and log files could be changed. In fact, there is little that could not be manipulated. It would be a potent attack.

195. A robust post-election audit of paper ballots is capable of detecting changes to the election results if the paper ballot is trustworthy. However, by statute, post-election audits in Georgia are rare, far too infrequent to offer a strong defense. Dr. Philip Stark has stressed this point and elaborated on the limitations of Georgia's paper ballots and post-election audits in his declarations in this case.¹³⁰

Greater Access Facilitates Deploying Weaponized Code

196. After developing techniques or weaponized code, an adversary must then gain access to election hardware with enough opportunity to put them into action. If hardware is not connected to a network, it requires physical access. Some of the obstacles to gaining physical access were described previously, such as access-restricted rooms, locks, and tamper-evident seals. As with obtaining the software, adversaries need sufficient resources to gain access with enough opportunity.

¹³⁰ Dr. Philip Stark, March 9, 2022 Expert Report, <https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-9.pdf>

197. Unfortunately, the Coffee County data breach portends a lower threshold for gaining that access. Election office staff invited in *strangers*, with no expertise in voting systems, and gave them free rein for hours. Software and data was copied and removed from the premises. Voting machines were studied as their operational settings were changed using a trial-and-error methodology. A vote tabulator was broken open and its inner parts scrutinized. Access-restricted rooms, passwords, locks, and tamper-evident seals offered no defense at all.

198. The SullivanStrickler team and others present on January 7, 2021 had access to Coffee County election hardware for over seven hours. The group worked without supervision by election officials. Misty Hampton, the Coffee County Election Director at the time, told *The Washington Post* she did not know where the group went or exactly what they did while they were there. “I’m not a babysitter,” she said.¹³¹

199. Based on their professional backgrounds, several individuals present that day, as well as on the seven days of subsequent visits, appear to have had sufficient access, skills, and opportunity to perform malicious manipulations—

¹³¹ Emma Brown and Amy Gardner, “Georgia County Under Scrutiny After Claim of Post-Election Breach”, *The Washington Post*, May 13, 2022.
<https://www.washingtonpost.com/investigations/2022/05/13/coffee-county-misty-hampton-election>

including variations of the [REDACTED] proof-of-concept attacks detailed in Dr. Halderman's report.¹³²

200. Many similar data breaches transpired around the country last year, often facilitated by insiders. I have logged 11 reported attempts in the United States since November 2020 to access election hardware to copy its data, 10 of which were successful. In one case, election hardware was taken away and returned six months later. Some election officials were willing participants. Some election officials were persuaded to give access by people who misrepresented the facts or their authority. In all of them, strangers gained unprecedented access to election hardware.

201. Similarly, the likelihood of manipulation attempts has risen. In the June 2022 primary in Pueblo County, Colorado, a Dominion ICX ballot marking device in a vote center alerted poll workers that it had detected a change to its USB devices. It is possible someone attempted to remove the legitimate USB drive or to install an unauthorized device. The *Associated Press* wrote, "The incident in Pueblo County highlights a troubling reality, that any voter propelled by

¹³² Dr. J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices*, 2021. (Sealed)

conspiracy theories could try to tamper with voting machines.”¹³³ In my view, it is a canary in the coal mine. I expect more attempts like it.

202. It is easier to gain access to election hardware and software now than it was only a few years ago, and disinformation has motivated ordinary people to test the limits of the system and to take risks they would not have attempted previously. Easier access and more motivation increases the number of adversaries who may try to tamper with election systems and increases the likelihood some will succeed in causing incidents.

Increased Risks Require Urgent Action

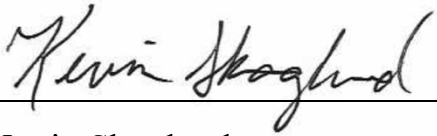
203. Security risk is measured in part by assessing the *likelihood* a negative incident will occur. Wide, uncontrolled availability of Georgia’s election software substantially increases the likelihood of an incident. Adversaries motivated by disinformation substantially increases the likelihood of an incident. Convenient access to Georgia’s election offices and hardware substantially increases the likelihood of an incident. Thus, the election security risks have increased substantially for every Georgia county.

204. Though the threat landscape has changed, the risk mitigations recommended by election security experts have not. They are: rigorous access

¹³³ Christina Cassidy and Colleen Slevin, “Voting Machine Tampering Points to Concern for Fall Election”, *Associated Press*, August 25, 2022, <https://apnews.com/article/2022-midterm-elections-voting-presidential-conspiracy-theories-colorado-53c90f7afe304e26eace79b4699181bb>

controls, layers of security defenses, resilience planning, hand-marked paper ballots, strong chain of custody of cast paper ballots, and robust post-election audits. These election best practices, cybersecurity controls, and the principles for evidence-based elections were developed with these threats in mind. Increased risks does not demand some new cure. It demands increased *urgency* for implementing the recommendations fully. The State of Georgia should act urgently and has not.

Executed on this date, December 5, 2022.


Kevin Skoglund